ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61069-5— 2017

ИЗМЕРЕНИЕ, УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ ПРОМЫШЛЕННОГО ПРОЦЕССА. ОПРЕДЕЛЕНИЕ СВОЙСТВ СИСТЕМЫ С ЦЕЛЬЮ ЕЕ ОЦЕНКИ

Часть 5

Оценка надежности системы

(IEC 61069-5:2016, IDT)

Издание официальное

Москва
Стандартинформ
2017

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Негосударственным образовательным частным учреждением дополнительного профессионального образования «Новая Инженерная Школа» (НОЧУ «НИШ») на основе собственного перевода на русский язык англоязычной версии указанного в пункте 4 стандарта, который выполнен Российской комиссией экспертов МЭК/ТК 65 и Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации (ВНИИНМАШ)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 306 «Измерения и управление в промышленных процессах»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 ноября 2017 г. № 1653-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61069-5:2016 «Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 5. Оценка надежности системы» (IEC 61069-5:2016 «Industrial-process measurement, control and automation — Evaluation of system properties for the purpose of system assessment — Part 5: Assessment of system dependability», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВЗАМЕН ГОСТ Р МЭК 61069-5—2012

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2017

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения, обозначения и сокращения 2
3.1 Термины и определения 2
3.2 Обозначения и сокращения 2
4 Основы оценки, связанные с надежностью 2
4.1 Свойства надежности 2
4.2 Факторы, влияющие на надежность 5
5 Процедура оценки 5
5.1 Общие положения 5
5.2 Определение целей оценки 5
5.3 Проектирование и схема оценки 5
5.4 Планирование программы проведения оценки 6
5.5 Проведение оценки 6
5.6 Отчет об оценке 6
6 Методы определения свойств 6
6.1 Общие положения 6
6.2 Аналитические методы определения свойств 7
6.3 Эмпирические методы определения свойств 8
6.4 Дополнительные вопросы методов определения свойств 9
Приложение А (справочное) Контрольный перечень и/или пример ДТС для надежности системы 10
Приложение В (справочное) Контрольный перечень и/или пример ДДС для надежности системы 11
Приложение С (справочное) Пример перечня пунктов оценки (информация из МЭК ТС 62603-1) . . . 12
Приложение D (справочное) Испытания достоверности 16
Приложение Е (справочное) Доступные базы данных интенсивности отказов 18
Приложение F (справочное) Требования обеспечения безопасности 19
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 21
Библиография 22

Введение

В МЭК 61069 рассматривается метод, который следует использовать для оценки системных свойств основной системы управления (ОСУ). МЭК 61069 состоит из следующих частей:

часть 1. Терминология и основные концепции;

часть 2. Методология оценки;

часть 3. Оценка функциональности системы;

часть 4. Оценка производительности системы;

часть 5. Оценка надежности системы;

часть 6. Оценка эксплуатабельности системы;

часть 7. Оценка безопасности системы;

часть 8. Оценка других свойств системы.

Оценка системы — основанное на доказательстве суждение о пригодности системы для определенного целевого назначения или класса целевых назначений.

Для получения полного итогового доказательства потребовалось бы полное (т. е. при всех влияющих факторах) определение пригодности всех свойств системы для конкретного целевого назначения или класса целевых назначений.

Так как на практике это требуется редко, для оценки системы более рациональным будет:

- определить критичность соответствующих свойств системы;
- спланировать определение (оценку) соответствующих свойств системы на основе экономического принципа «цена — целесообразность» для усилий по реализации этих свойств.

При проведении оценки системы следует стремиться к получению максимальной обоснованности пригодности системы с учетом целесообразной стоимости и ограничений по времени.

Оценка может быть выполнена только в том случае, если целевое назначение (миссия) сформулировано (или задано), или если оно может быть представлено гипотетически. В случае отсутствия миссии оценка не может быть выполнена. Тем не менее, возможно определение свойств системы в части сбора и систематизации данных для последующей оценки, проводимой другими лицами. В таком случае настоящий стандарт может применяться как руководство для планирования, а также устанавливает процедуры определения свойств системы, являющиеся неотъемлемой частью оценки системы.

При подготовке к оценке может быть установлено, что определение границ системы является слишком узким. Например, для средства с двумя или более версиями совместного пользования системы управления, например сети, необходимо учитывать вопросы сосуществования и функциональной совместимости. В этом случае система, подлежащая оценке, не должна ограничиваться «новыми» ОСУ. Такая система должна включать в себя как «новые», так и «старые» системы. То есть, система должна изменять свои границы, чтобы включать в себя достаточный объем другой системы для решения требуемых от нее задач.

Структура настоящей части и ее взаимосвязь с другими частями МЭК 61069 показаны на рисунке 1.



Рисунок 1 — Общий состав МЭК 61069

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИЗМЕРЕНИЕ, УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ ПРОМЫШЛЕННОГО ПРОЦЕССА. ОПРЕДЕЛЕНИЕ СВОЙСТВ СИСТЕМЫ С ЦЕЛЬЮ ЕЕ ОЦЕНКИ

Часть 5

Оценка надежности системы

Industrial-process measurement, control and automation. Evaluation of system properties for the purpose of system assessment. Part 5. Assessment of system dependability

Дата введения — 2018—09—01

1 Область применения

Настоящий стандарт:

- устанавливает детальный метод оценки надежности основной системы управления (ОСУ) на основании общих концепций, данных в МЭК 61069-1, и методологии оценки, приведенной МЭК 61069-2;
- устанавливает основную классификацию свойств надежности;
- описывает факторы, влияющие на надежность, и которые необходимо учитывать при оценке надежности; и
- предоставляет руководство по выбору методов из набора вариантов (с нормативными ссылками) для определения надежности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта. Для недатированных ссылок применяют последнее издание ссылочного стандарта (включая все изменения к нему).

IEC 60300-3-2, Dependability management — Part 3-2: Application guide — Collection of dependability data from the field (Управление надежностью. Часть 3-2. Руководство по применению. Сбор данных по надежности с места эксплуатации)

IEC 60319, *Presentation and specification of reliability data for electronic components* (Представление и спецификация данных о надежности электронных компонентов)

IEC 61069-1:2016, Industrial-process measurement, control and automation — Evaluation of system properties for the purpose of system assessment — Part 1: Terminology and basic concepts (Измерение и управление промышленным процессом. Определение свойств системы с целью ее оценки. Часть 1. Общие подходы и терминология)

IEC 61069-2:2016, Industrial-process measurement, control and automation — Evaluation of system properties for the purpose of system assessment — Part 2: Assessment methodology (Измерение и управление промышленным процессом. Определение свойств системы с целью ее оценки. Часть 2. Методология оценки)

IEC 61070, Compliance test procedures tor steady-state availability (Сравнение процедур проверки на установленную готовность)

Издание официальное

IEC 61709:2011, Electric components — Reliability — Reference conditions for failure rates and stress models for conversion (Компоненты электронные. Надежность. Стандартные условия для интенсивности отказов и нагрузочные модели для преобразования)

ISO IEC 25010, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models [Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов]

ISO IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования)

ISO IEC 27002, Information technology — Security techniques — Code of practice for information security controls (Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности)

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по МЭК 61069-1.

3.2 Обозначения и сокращения

В настоящем стандарте применены обозначения и сокращения по МЭК 61069-1.

4 Основы оценки, связанные с надежностью

4.1 Свойства надежности

4.1.1 Общие положения

Для обеспечения полной оценки надежности системы системные свойства необходимо, прежде всего, классифицировать в иерархическом порядке.

Для того чтобы система была надежной, необходимо, чтобы она была готова выполнить свои функции. Однако на практике это не означает, что, если система готова выполнить свою функцию, то, функция будет выполнена правильно.

Для того чтобы раскрыть эти два аспекта, свойства надежности подразделены на группы и подгруппы, приведенные на рисунке 2.

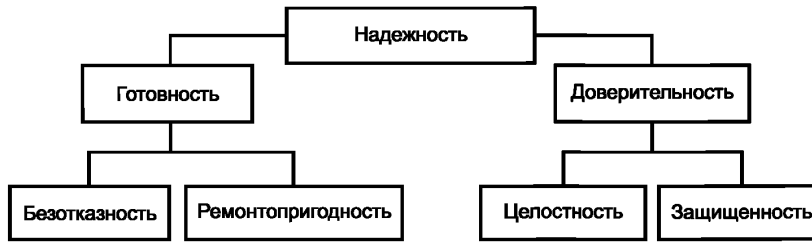

Рисунок 2 — Составляющие свойства надежности

Надежность системы не может быть оценена непосредственно и определена по одному свойству. Надежность системы может быть определена только при помощи анализа и испытания каждого ее свойства по отдельности.

Взаимосвязь между свойствами надежности системы и ее модулями иногда бывает очень сложной.

Например:

- если конфигурация системы включает резервирование, готовность системы зависит от свойства целостности избыточных модулей;
- если конфигурация системы содержит механизмы защищенности системы, свойство защищенности системы зависит от свойства готовности модулей, которые реализуют механизм защиты;
- если конфигурация системы содержит модули, которые проверяют данные, передаваемые от других частей системы, то целостность системы зависит от свойств защищенности этих модулей.

Если система выполняет несколько системных задач, ее надежность может очень сильно влиять на эти задачи. Поэтому для каждой из этих задач требуется проведение отдельного анализа.

4.1.2 Готовность

Готовность системы зависит от готовности отдельных модулей системы и способа, которым эти модули взаимодействуют при выполнении задач системы. Способ, которым обеспечивается взаимодействие модулей, может включать функциональное резервирование (однородное или разнообразное), функциональный возврат и деградацию. Готовность, как правило, зависит от применяемых процедур и ресурсов, доступных для поддержания системы. Готовность системы может отличаться для каждой из ее задач.

Готовность системы может отличаться в отношении каждой из ее задач.

Готовность системы для каждой задачи может быть определена количественно двумя способами.

Прогнозируемое значение готовности системы, может быть рассчитано по формуле:

$$\text{Готовность} = \frac{\text{среднее время до отказа}}{\text{среднее время до отказа} + \text{среднее время восстановления}},$$

где: - «готовность» — означает готовность системы к выполнению данной задачи;

- «среднее время до отказа» — означает среднее время с момента восстановления системы в состояние готовности выполнения данной задачи до момента времени, когда система будет не в состоянии ее выполнять (до отказа);
- «среднее время восстановления» — среднее время, необходимое для восстановления системы в состояние готовности выполнения заданной задачи с момента времени, когда система не смогла выполнить задачу.

Для системы, находящейся в эксплуатации, готовность может быть рассчитана по формуле:

$$\text{Готовность} = \frac{\text{время, за которое система в состоянии выполнить задачу}}{\text{время, за которое система, как ожидалось, выполнит задачу}}.$$

4.1.3 Безотказность

Безотказность системы зависит от безотказности отдельных модулей системы и способа, которым эти модули взаимодействуют при выполнении задачи системы. Способом, взаимодействия модулей может быть функциональное резервирование (однородное или многообразное), функциональный возврат и ухудшение функционирования.

Безотказность системы может быть различной для каждой из ее задач. Безотказность может быть определена количественно для отдельных задач с различными степенями предсказуемой доверительности.

Безотказность отдельных элементов системы может быть предсказана методом расчета безотказности составных частей данной системы (см. МЭК 62380 и МЭК 61069-6). В этом случае, безотказность системы может быть предсказана синтезом. Следует отметить, что для модулей программного обеспечения систем нет доступных методов предсказания безотказности, которые обеспечивают высокий уровень доверительности.

Механизмы анализа безотказности программного обеспечения описаны в ИСО МЭК 25010.

Безотказность может быть выражена средним временем до отказа или интенсивностью отказов.

4.1.4 Ремонтопригодность

Ремонтопригодность системы зависит от ремонтопригодности отдельных элементов, структуры элементов и модулей системы. Физическая структура устанавливает легкость доступа, заменяемость и т. д. Функциональная структура устанавливает простоту диагностики и т. д.

При количественном определении ремонтопригодности системы, должны быть учтены все действия, требуемые для восстановления состояния системы, в котором она способна полностью выполнять задачи. Также должны быть учтены затраты времени, которые необходимы для обнаружения ошибки, подготовки к техобслуживанию и ремонту, проведения диагностики и исправления причины отказа, настройки и проверки, и т. д.

Количественное определение ремонтопригодности следует дополнять качественными путем проверки обеспечения и учета следующих моментов:

- оповещение о возникновении отказов: световая сигнализация, аварийные сообщения, отчеты и т. д.;
- доступ: простота доступа для персонала и для подключения измерительных приборов, модулей и т. д.;
- диагностика: прямая идентификация ошибки, диагностические инструменты, которые не оказывают никакого влияния на систему, удаленные средства поддержки обслуживания, статистическая ошибка проверки и передачи сообщений;
- ремонтопригодность/заменяемость: несколько ограничений на замену модулей во время эксплуатации (поддержка «горячей» замены), модульный принцип, однозначная идентификация модулей и элементов, минимальная потребность в специальных инструментах, минимальные последствия для других элементов или модулей, при замене элементов или модулей;
- контроль: инструкции по процедурам обслуживания, минимальные требования контроля.

Ремонтопригодность может быть представлена посредством среднего времени восстановления.

4.1.5 Достоверность

Достоверность системы зависит от целостности и механизмов защищенности, реализуемых как функции, выполняемые модулями системы.

Механизмы достоверности включают:

- проверку:
  - правильности выполнения функций (например, устройством обеспечения безопасности с использованием известных данных); и/или
  - корректности данных (например, проверка правильности, контроль по четности, обратное считывание, проверка вводимых значений и т. д.);
- операции типа:
  - самонастройка;
  - защита данных;
  - извещение об операции и т. д.

Данные и механизмы могут быть использованы для обеспечения целостности и/или защищенности.

Для анализа механизмов достоверности могут использоваться методы внесения ошибки, приведенные в подразделе 6.1.

Достоверность детерминирована, и поэтому некоторые аспекты могут быть определены количественно.

4.1.6 Защищенность

Защищенность системы зависит от механизмов, применяемых на границе системы, чтобы обнаружить и предотвратить некорректные входные сигналы и несанкционированный доступ. Такие границы могут быть физическими или виртуальными. Смотреть:

- приложение F для получения дополнительных рекомендаций по вопросам безопасности;
- стандарты МЭК серии 62443.

Механизм защищенности может быть реализован путем проверки элементом вводимых значений в другие элементы.

4.1.7 Целостность

Целостность зависит от механизмов, применяемых в выходных элементах системы для проверки корректности выходных сигналов. Целостность также зависит от механизмов, действующих в пределах системы для обнаружения и предотвращения некорректных передач сигналов или данных между частями системы.

Целостность детерминирована, и поэтому некоторые аспекты могут быть определены количественно.

Механизм целостности реализуется путем проверки элементом выводимых значений других элементов.

4.2 Факторы, влияющие на надежность

На надежность системы могут оказать воздействие влияющие факторы, перечисленные в подразделе 5.3 МЭК 61069-1:2016.

Для каждого свойства системы, указанного в подразделе 4.1, основными влияющими факторами являются:

- надежность: может быть подвержена воздействию влияющих факторов, исходящих из:
  - средств обеспечения, влияние частично предсказуемо при применении МЭК 61709,
  - окружающей среды, влияние частично предсказуемо, при применении МЭК 61709,
  - услуг, связанных с техническим обслуживанием, хранением частей и т. д.;
- ремонтопригодность: для целей настоящего стандарта, ремонтопригодностью считается внутреннее свойство самой системы, на которую оказывается непрямое воздействие, например, ограниченный доступ в результате воздействия опасных условий;
- готовность: принимая во внимание деятельность человека, необходимую для поддержания или восстановления системы в состоянии, в котором система способна выполнять требуемую задачу. Находится под влиянием поведения человека и условий обслуживания (задержка поставки запасных частей, обучение, документирование и т. д.);
- достоверность: на такие механизмы как защищенность и целостность могут воздействовать преднамеренные или непреднамеренные действия человека, нашествие вредителей. Если при этом используются обычные средства обслуживания типа шин или многозадачных процессоров, то эти механизмы могут находиться под влиянием задач системы, из-за внезапного возрастания активности промышленного процесса (например, при аварийной ситуации) и т. д., а также внешних систем.

В целом, любые отклонения от рекомендованных состояний, в которых система, как предполагается, будет работать, могут оказать влияние на правильность функционирования системы.

При проведении конкретных испытаний для определения результатов воздействия влияющих условий следует применять следующие стандарты:

- МЭК 60068;
- МЭК 60801;
- МЭК 61000;
- МЭК 61326.

5 Процедура оценки

5.1 Общие положения

Оценку следует проводить в соответствии с методологией, приведенной разделе 5 МЭК 61069-2:2016.

5.2 Определение целей оценки

Определение цели оценки следует проводить в соответствии с процедурами, приведенными в 5.2 МЭК 61069-2:2016.

5.3 Проектирование и схема оценки

Проектирование и схему оценки следует выполнять в соответствии с процедурами, приведенными в подразделе 5.3 МЭК 61069-2:2016.

Определение объема оценки следует проводить в соответствии с 5.3.1 МЭК 61069-2:2016.

Сопоставление документированной информации следует проводить в соответствии с 5.3.3 МЭК 61069-2:2016.

Заключения, сформулированные в соответствии с 5.3.3 МЭК 61069-2, должны содержать следующую информацию в дополнение к пунктам, перечисленным в 5.3.3 МЭК 61069-2:2016:

- дополнительные пункты не отмечены.

Документирование информации для сопоставления следует проводить в соответствии с 5.3.4 МЭК 61069-2.

Выбор элементов оценки должен производиться в соответствии с 5.3.5 МЭК 61069-2:2016.

Спецификация оценки должна быть разработана в соответствии с 5.3.6 МЭК 61069-2:2016.

Сравнение ДТС и ДСС следует проводить в соответствии с подразделом 5.3 МЭК 61069-2.

Примечание 1 — Контрольный перечень ДТС для определения надежности системы приведен в приложении А.

Примечание 2 — Контрольный перечень ДСС для определения надежности системы приведен в приложении В.

5.4 Планирование программы проведения оценки

Планирование программы проведения оценки следует выполнять в соответствии с методом, изложенном в подразделе 5.4 МЭК 61069-2:2016.

Действия по оценке должны быть разработаны в соответствии с 5.4.2 МЭК 61069-2:2016.

Итоговая программа проведения оценки должна определять пункты, перечисленные в 5.4.3 МЭК 61069-2:2016.

5.5 Проведение оценки

Оценки следует проводить в соответствии с подразделом 5.5 МЭК 61069-2:2016.

5.6 Отчет об оценке

Отчет об оценке следует оформлять в соответствии с подразделом 5.6 МЭК 61069-2:2016.

Отчет должен содержать информацию, приведенную в подразделе 5.6 МЭК 61069-2:2016. Дополнительно отчет по оценке должен включать в себя следующие пункты:

- дополнительные пункты не отмечены.

6 Методы определения свойств

6.1 Общие положения

В настоящем стандарте приведено несколько методов определения свойств. Могут применяться и другие методы, однако в этом случае в отчете об оценке следует указывать ссылки на документы, в которых описано применение таких методов.

Данные методы определения свойств сгруппированы согласно требованиям, установленным в разделе 6 МЭК 61069-2:2016.

Следует учитывать факторы, влияющие на свойства надежности системы, в соответствии с 4.2.

Методы, указанные в подразделах 6.2, 6.3 и 6.4, рекомендованы для оценки свойств надежности системы.

Количественное определение свойств может быть основано на прогнозирующем анализе, расчетах или на испытаниях.

Для того, чтобы начать оценку необходимо проанализировать функциональную и физическую структуру системы. После этого необходимо провести анализ выполнения задач системой.

Структура системы может быть описана с использованием схем функциональных и физических блоков, схем маршрутов прохождения сигналов, графов состояний, таблиц и т. д.

Режимы отказа рассматриваются для всех элементов системы (технических средств и программного обеспечения) и определяется их влияние на надежность выполнения задач системы, а также на требования к ремонтопригодности.

Качественный анализ может быть выполнен с применением одного или комбинации методов, описанных в подразделах 6.2 и 6.3.

Анализ должен включать проверку способа, которым в системе инициируются альтернативные пути, то есть:

- статическим способом с изменением конфигурации системы; или
- динамическим или автоматическим, например, механизмами достоверности или вручную, например, через клавиатуру.

Перечень аспектов, которые должны быть учтены при оценке, приведен в МЭК 60319 и МЭК 61709. Аналитические методы, описанные ниже, основаны на моделях. Такие модели редко могут представлять реальную систему достаточно точно, и даже в этом случае, нельзя быть уверенным в том, что достигнуто 100 %-ное сходство. Поэтому результаты, основанные на аналитических методах, следует также дополнять данными о степени их достоверности.

Надежность системы зависит также от ошибок на стадиях проектирования, спецификации и производства системы. Это одинаково справедливо для технических средств и программного обеспечения системы. Данные ошибки могут быть обнаружены только при тщательной проверке и надлежащем выполнении каждой функции.

Кроме того, применяется внесение гипотетических отказов или ошибок в систему, которые являются методическими, для увеличения степени доверительности при окончательной оценке надежности готовой системы, которая достигается на протяжении всех этапов проектирования, спецификации и производства системы. Такие методы внесения ошибок могут быть выполнены с использованием средств автоматизации и/или специально разработанных программ. Они применяются для того, чтобы выявить, каковы могут быть последствия от гипотетических отказов или ошибок для задач системы.

Тем не менее, необходимо признать, что на практике увеличение степени достоверности ограничено, так как число испытаний, которые могут быть запланированы и выполнены, будет ограничено числом всех возможных отказов и ошибок, которые можно ожидать и, кроме того, ввести дополнительно.

Примечание — Пример перечня элементов приведен в приложении С.

6.2 Аналитические методы определения свойств

6.2.1 Общие положения

В данном подразделе обсуждается общая методика аналитической оценки: логический анализ (индуктивный и дедуктивный) и прогностическая оценка.

6.2.2 Индуктивный анализ

Режимы отказа идентифицируются на уровне компонента или элемента, и для каждого из этих режимов анализируется на более высоком уровне соответствующее влияние на надежность выполнения задач системы. Результирующее воздействие отказа приводит к режимам отказа на следующем более высоком уровне.

Этот подход «снизу-вверх» — трудоемкий метод, заканчивающийся идентификацией воздействий на всех уровнях системы для всех постулированных режимов отказов.

Соответствующий индуктивный метод анализа описан в МЭК 60812.

6.2.3 Дедуктивный анализ

При дедуктивном анализе рассматривается гипотетический отказ на самом высоком уровне системы, то есть отказ выполнения задачи с последовательным рассмотрением более низких уровней.

Следующий более низкий уровень анализируется для идентификации режимов отказа и связанных отказов, которые привели бы к идентифицированному отказу на самом высоком уровне, то есть на уровне задачи.

Анализ повторяется с прослеживанием обратного прохождения через функциональные и физические части системы до тех пор, пока анализ не приведет к получению достаточной информации для оценки в отношении надежности (включая ремонтопригодность).

Дедуктивный анализ не дает никакой информации относительно режимов отказа, которые не рассматриваются как события. Тем не менее, его применение очень эффективно по временным затратам для сложных систем, для которых более удобно описать то, что называется отказом системы или успешным выполнением задачи, чем рассматривать все возможные режимы отказов составляющих элементов системы.

Соответствующий дедуктивный метод анализа описан в МЭК 61025.

6.2.4 Прогнозируемое определение свойства

Прогнозируемое определение свойства основано на анализе качественных характеристик, дополненном определением количественной оценки безотказности (интенсивности отказов) элементов системы. Чтобы определить интенсивность отказов системы при выполнении задач, требуется применение прогнозирующего анализа. Соответствующий метод описан в МЭК 61078.

Схема безотказности блока может быть построена, как правило, непосредственно исходя из функциональной и физической структур системы. Метод направлен, прежде всего, на анализ успешного выполнения задачи (с двумя устойчивыми состояниями) и не касается влияния ни сложного ремонта, ни стратегий обслуживания, ни других ситуаций с несколькими устойчивыми состояниями.

Различные математические инструменты пригодны для вычисления интенсивности отказов — типа булевой алгебры, таблиц истинности и/или траектории и анализа секущего множества. Для количественного прогноза интенсивности отказов системы при выполнении задачи в ситуации, характеризующейся большим числом состояний, может использоваться методика Маркова, описанная в МЭК 61165.

Тем не менее, применение методики Маркова становится очень сложным, если необходимо рассмотреть большое число состояний системы. В таких случаях более эффективно применить анализ Маркова для расчета данных по безотказности для подгрупп моделей анализа, полученных одним из других методов анализа, например, таким как «анализ дерева неисправностей».

Основные количественные данные по интенсивности отказов модулей и элементов, используемых в вышеупомянутых методах анализа, могут быть получены из опыта эксплуатации или методом «прогнозирования безотказности частей», используя общие данные для компонентов модулей и элементов. Метод прогнозирования безотказности частей описан в МЭК 61709.

Для учета уровня стресса в результате влияющих факторов необходимо использовать метод, описанный в МЭК 61709, а также информацию, указанную в приложении А.

Метод учета частей основан на предположении, что компоненты функционально связаны в последовательном порядке (худшая оценка события). Компоненты модулей и элементов системы внесены списком в модуль или элемент, установленный для каждого компонента этого типа, соответствующий ему поток отказов, факторы, влияющие на интенсивность отказов (качество части, окружающая среда и т. д.) и обычно порядковый номер.

В качестве альтернативы общие данные об отказах можно найти в ссылках, содержащихся в приложении Е.

Для сложных систем, таких как ОСУ, на практике невозможно сделать точный прогноз оценки свойств надежности.

Свойства системы — ремонтопригодность, защищенность, и целостность — зависят, главным образом, от особенностей проектируемой системы, и, следовательно, степень их осуществления не может быть рассчитана на основе вероятностного подхода. Должна быть рассмотрена безотказность элементов, используемых для оценки защищенности и целостности. Методы, которыми обычно оценивалась надежность этих элементов, могут быть теми же самыми, ввиду того, что они применялись для элементов и модулей, поддерживающих основные функции системы.

6.3 Эмпирические методы определения свойств

6.3.1 Общие положения

Полагаться исключительно на этап испытания системы, чтобы измерить безотказность и готовность сложной системы, не является ни практически реализуемым, ни рентабельным. В целом, сложные системы уникальны (особенно когда образец существует в единственном экземпляре). Кроме того, объем таких испытаний будет ограничен по обеспечению и строго ограничен по времени, отводимому для испытаний. Однако, для систем, которые уже эксплуатируются, такие испытания представляют ценную информацию.

Полученные при этом фактические данные полезны для:

- совершенствования будущих проектов, структуры системы, модернизации или замены устаревшего оборудования и программного обеспечения;
- сравнения с ожидаемыми или заданными характеристиками;
- использоваться для прогнозирования показателей надежности.

Руководство по процедурам, которым нужно следовать при определении испытаний, можно найти в МЭК 61070 и МЭК 60300-3-2.

Главная цель проведения испытаний систем состоит в том, чтобы определить поведение системы (технических средств и программного обеспечения) при возникновении ошибки или несанкционированного или неправильного доступа (защищенность и целостность).

Для того чтобы наблюдать поведение системы должна быть определена типовая задача или конкретный набор задач, и для каждой задачи установлены состояния системы, которые рассматриваются как отказ (например, состояние выходов). Руководство по проведению таких испытаний приведено в МЭК 60706-4.

6.3.2 Испытания методами внесения ошибки

Перед проведением испытания методом внесения ошибки, должна быть исследована спецификация системы, чтобы определить:

- мероприятия по обеспечению целостности, предотвращающие распространение ошибок внутри систем;
- мероприятия по защищенности, предотвращающие ошибочные или несанкционированные вхождения в систему;

- наличие диагностических возможностей.

Для эффективного по времени проведения испытаний проект испытаний системы должен быть основан на анализе качественных характеристик и, насколько возможно, должен использовать диагностические возможности, предусмотренные в самой системе и пригодные для системы. Когда диагностические возможности необходимы для обеспечения надежности системы, должна быть проявлена осторожность, и сами эти возможности должны пройти отдельную проверку.

Для проверки целостности ошибки могут быть внесены в модули, элементы и/или компоненты, и проведены наблюдения за тем действительно ли:

- отказывают выходы системы; и/или
- имеется сообщение об ошибке.

Чтобы проверить защищенность, в систему могут быть внесены ошибки или несанкционированная информация, то есть поступили некорректные входные данные, совершена ошибка в действиях человека при эксплуатации и/или обслуживании.

При проверке целостности и защищенности должна быть проявлена осторожность при проведении некоторых одновременных испытаний. Результатом некоторых отказов могут стать отсутствие обнаружения отказов, то есть, неопределяемый отказ. Поэтому необходимо проявлять осторожность при включении одновременных испытаний целостности и защищенности. В приложении D приведен ряд ошибок, которые могут быть обнаружены при проведении этих испытаний.

6.3.3 Испытания влияния окружающей среды

Некоторые воздействия влияющих условий могут вызывать срабатывание механизмов обеспечения защищенности.

Поэтому выбранные влияющие факторы должны быть различными относительно их нормальных значений для того, чтобы проверить механизмы защищенности.

Для выбора влияющих факторов следует обратиться к подразделу 4.2.

6.4 Дополнительные вопросы методов определения свойств

Дополнительные пункты не отмечены.

Приложение А
(справочное)

Контрольный перечень и/или пример ДТС для надежности системы

Документ о требованиях к системе должен проходить проверку, чтобы убедиться, что для каждой системной задачи четко определено нижеследующее:

- относительная важность такой задачи;
- определение того, что считается отказом задачи;
- критерии отказа в отношении свойств надежности;
- рабочая и операционная среда.

Спецификация отказа в количественном или качественном выражении должна соответствовать формату, определенному до начала анализа и оценки.

Приложение В
(справочное)

Контрольный перечень и/или пример ДДС для надежности системы

В.1 Информация ДДС

Документ спецификации системы необходимо проверять на соответствие свойств, указанных в ДДС, требованиям МЭК 61069-2:2016, приложение В.

В.2 Контрольный перечень для надежности системы

Особое внимание следует уделить проверке предоставления информации в отношении:

- функций системы, поддерживающих каждую задачу, модулей, элементов, технических средств и программного обеспечения, обеспечивающих реализацию каждой из этих функций;
- альтернативных маршрутов, поддерживаемых системой для выполнения каждой задачи, и способов их активации;
- механизмов обеспечения достоверности (защищенности и целостности) и способов их поддержки;
- безотказности и готовности каждой задачи, а также функций поддержки, модулей и элементов;
- характеристик ремонтопригодности;
- эксплуатационных характеристик, свойств окружающей среды и границ применения модулей и элементов.

Приложение С
(справочное)

Пример перечня пунктов оценки (информация из МЭК ТС 62603-1)

С.1 Общие положения

Настоящее приложение содержит несколько примеров влияющих факторов, имеющих отношение к данной части МЭК 61069, которые были взяты из МЭК ТС 62603-1.

Классификации значений свойств, описанных в данном документе, приведены только в качестве примеров.

С.2 Надежность

Надежность не может быть описана просто количественно (числом). Некоторые из ее свойств могут быть выражены как вероятности, другие свойства детерминированы; некоторые могут быть определены количественно, другие аспекты могут только быть описаны качественным способом.

Когда система выполняет несколько системных задач, ее надежность может очень сильно влиять на эти задачи. Поэтому для каждой из этих задач требуется отдельный анализ.

С.3 Готовность

С.3.1 Самодиагностика системы

Самодиагностика системы позволяет быстро выявить ошибку и тем самым сократить среднюю продолжительность ремонта. По этой причине, оценщик должен учесть возможности самодиагностики системы на всех ее уровнях.

Может понадобиться выполнить процедуры самодиагностики основных компонентов ОСУ, таких как платы ввода/вывода или модули, процессорная плата, карты памяти и линии связи.

Самодиагностика полевых устройств должна выполняться в логике управления для активации функций безопасности или восстановления действия в случае возникновения полевых ошибок. Самодиагностика других компонентов ОСУ является частью системы управления аварийными сигналами.

С.3.2 Устойчивость к отказам и резервирование дискретного компонента

С.3.2.1 Общие положения

Устойчивость к отказам представляет собой встроенную способность системы обеспечивать длительное и правильное выполнение заданных функций при наличии аппаратного или программного сбоя дискретного компонента. Другими словами, система способна выполнять свое целевое назначение (миссию) даже после первого сбоя (аппаратного или программного).

С.3.2.2 Критерии резервирования

При определении системы управления, должны быть оценены влияния отказа компонента по отношению к контролируемому процессу, а также резервирование должно быть запрошено соответствующим образом.

Резервирование должно охватывать компоненты, которые являются критичными или важными для правильной и безопасной работы всей системы. При определении критериев резервирования должны быть учтены следующие требования, если это применимо, в соответствии с типом компонента:

- тип режима ожидания, при наличии;
- управление программным обеспечением и резервное копирование данных между резервными компонентами;
- политика резервирования (1 из 2, 2 из 3, *k* из *m*);
- синхронизация данных между активными и резервными машинами;
- конфигурация активной и резервной машины.

Это особенно целесообразно для определения наличия устойчивости к отказам и/или резервирования в:

- источнике питания, включая резервный источник бесперебойного питания (ИБП);
- модулях ввода/вывода;
- сетях ввода/вывода между модулями ввода/вывода и контроллерами;
- контроллерах;
- управляющих сетях, соединяющих элементы управления, рабочие станции и другие компоненты;
- рабочих местах операторов, которые, например, могут заменить любую рабочую станцию;
- серверах.

Характеристики важности включают:

- плавное восстановление после отказа;
- время восстановления после отказа (время, когда услуга не доступна);
- режимы отказа (несколько режимов отказа могут вызвать потерю первичного и вторичного отказа).

С.3.3 Методы резервирования

С.3.3.1 Общие положения

Готовность системы зависит от готовности отдельных частей системы и способа, которым эти части взаимодействуют при выполнении задач системы. Способ, которым обеспечивается взаимодействие частей, может включать:

- функциональное резервирование (однородное или многообразное): резервирование конкретной функции можно получить при использовании одинаковых аппаратных средств как для основных, так и резервных (однородных) или независимых аппаратных средств (многообразных). Если функциональное резервирование доступно, первый отказ не приводит к снижению функциональных возможностей и производительности системы;
- функциональный возврат: это способность возврата к известному функциональному уровню или режиму в случае отказа или ненормальной работы;
- ухудшение функционирования: в случае отказа части ОСУ, снижаются производительность и функциональность системы. При ухудшенном рабочем состоянии все критические функции работают правильно.

Готовность зависит от используемых методик и имеющихся ресурсов для поддержания системы. Требования к готовности, как правило, выражаются в виде суммарного времени простоя, возникающего в течение определенного периода времени. Для различных задач ОСУ возможны различные значения готовности.

В дополнение к необходимому времени простоя, дополнительные конкретные требования, в соответствующих случаях, должны быть определены для увеличения готовности некоторых важных функций в отношении резервирования компонента.

С.3.3.2 Допустимые условия ухудшения качества функционирования

Из-за ошибок в системе вся система не может достигнуть выполнения всех функций, которые представляют ее целевое назначение (миссию). Если ухудшенные рабочие условия являются допустимыми, можно поддерживать процесс и систему в рабочем состоянии даже после прекращения работы одной или нескольких функций. Необходимо определить, какие функции не являются критическими для функционирования системы, и какие могут быть потеряны в ухудшенных условиях. Способность работать в ухудшенных условиях повышает готовность ОСУ.

С.3.3.3 Резервные конфигурации

Если некоторые критические компоненты являются резервными, необходимо определить резервные конфигурации.

В принципе, существует два возможных режима резервной конфигурации:

- горячее резервирование: основной и резервный компоненты или системы работают одновременно. Данные, если компонент должен их обрабатывать, воспроизводятся на резервном компоненте в режиме реального времени таким образом, что два компонента становятся идентичными. Система может выполнить горячую замену между первичным и резервным компонентом без потери данных;
- холодное резервирование: в этой конфигурации резервный компонент вызывается только тогда, когда первичный компонент не срабатывает. Данные, в случае необходимости, воспроизводятся в резервном компоненте с более низкой скоростью обновления, чем в случае горячего резервирования. Эта конфигурация используется для некритических применений.

Между горячим и холодным резервированием могут существовать промежуточные решения, которые иногда именуются как «теплое резервирование».

С.3.3.4 Защитное действие отказоустойчивого режима

Понятие «отказоустойчивый режим» означает защиту от воздействия отказа оборудования. Отказоустойчивый режим относится к способности переключения в заданное безопасное состояние при возникновении конкретного сбоя. Для выполнения отказоустойчивой защиты необходимо определить отказоустойчивые устройства (т. е. компоненты, системы, устройства управления и т. д.), которые разработаны с возможностью установления контролируемых параметров в заданном (безопасном) состоянии при обнаружении отказа.

Следует определить действия, которые отказоустойчивое устройство реализует при запросе срабатывания в качестве отказоустойчивого устройства. Например, для отказоустойчивого клапана, защитным действием может быть открытое или закрытое положение.

С.3.3.5 Компоненты, заменяемые в горячем режиме

Каждый компонент ОСУ считается заменяемым в горячем режиме, если он может быть удален и заменен во время работы ОСУ. ОСУ автоматически настраивает новый компонент, в соответствии с настройками удаленного компонента. Горячая замена возможна как с неисправными, так и с исправными компонентами. Возможность горячей замены часто требуется для критически важных компонентов, отказ которых может поставить под угрозу одну или несколько функций ОСУ. По этой причине компоненты с возможностью замены в горячем режиме, как правило, имеют установленные резервные компоненты. В технических условиях ОСУ должны быть указаны критические компоненты, для которых необходим режим горячей замены (при наличии).

С.4 Безотказность

Безотказность системы зависит от безотказности отдельных модулей системы и способа, которым эти модули взаимодействуют при выполнении задачи системы. Способом взаимодействия модулей может быть функциональное резервирование (однородное или многообразное), функциональный возврат и ухудшение функционирования. Безотказность системы может быть различной для каждой из ее задач. Безотказность может быть определена

количественно для отдельных задач с различными степенями предсказуемой доверительности. Безотказность отдельных частей аппаратных средств системы может быть предсказана методом расчета безотказности составных частей данной системы (см. МЭК 62380). Безотказность всей системы может быть рассчитана при помощи аналитических средств и методов (см. МЭК 61078 и МЭК 61025). Следует отметить, что для модулей программного обеспечения систем нет доступных методов предсказания безотказности, которые обеспечивают высокий уровень доверительности.

С.5 Ремонтопригодность

С.5.1 Общие положения

Ремонтопригодность — это способность элемента сохранять или восстанавливать в заданных условиях эксплуатации такое состояние, в котором оно выполняет требуемую функцию, если в этих условиях проводится его техническое обслуживание с использованием установленных процедур и ресурсов.

С.5.2 Формирование запросов на сопровождение

Система может формировать запросы на сопровождение при изменении рабочего состояния компонента. Способность формирования запроса на сопровождение является способом проведения планово-предупредительного сопровождения. Устройства или подсистемы автономно определяют необходимость проведения ремонта до возникновения сбоев. Такая способность в основном связана с интеллектуальными полевыми устройствами, такими как аналитические инструменты, позиционеры клапанов и т. д.

С.5.3 Стратегии сопровождения

Существуют следующие различные стратегии сопровождения:

- корректирующее сопровождение: реакция на существующий сбой и диагностические сообщения. В данном значении сопровождение означает ремонт или замену поврежденного элемента;
- профилактическое сопровождение: надлежащие меры по сопровождению инициируются до возникновения сбоя. В данном значении сопровождение означает выполнение зависящей от времени или состояния политики ремонта или замены;
- планово-предупредительное сопровождение: предупредительная диагностика для своевременного выявления потенциальных проблем и определения оставшегося срока службы. В данном значении сопровождение означает планирование соответствующего ремонта или замены на основании измеренных данных.

В определении требований должны быть определены требуемые стратегии обслуживания.

С.5.4 Сопровождение программного обеспечения системы

В соответствии с ИСО МЭК 14764 сопровождение программного обеспечения представляет собой модификацию программного продукта после устранения неисправностей с целью улучшения производительности и других свойств или адаптирования продукта к модифицированной среде.

Сопровождение программного обеспечения ОСУ включает в себя установку заплат, обновлений или новых версий программно-аппаратных средств.

Потребитель должен требовать от подрядчика услугу обновления программного обеспечения. Данная услуга включает в себя любые новые версии (основная или дополнительная, в зависимости от условий контракта) или заплату, разработанную подрядчиком в течение периода технического обслуживания.

Услуга обновления программного обеспечения может ограничиваться исключительно поставкой новых версий и заплат или может также включать в себя установку модернизированного программного обеспечения на саму систему.

Подрядчик должен уведомить пользователя о совместимости всех основных официальных заплат операционной системы или обновлений для системы безопасности в самой системе. При необходимости, потребитель должен также включить в услугу обновления программного обеспечения установку официальных заплат операционной системы и обновлений системы безопасности.

С.6 Достоверность

Достоверность зависит от:

- способности системы давать предупреждающий сигнал при возникновении состояния, в котором она не способна правильно (безошибочно) выполнять некоторые или все свои функции;
- способности системы отклонять любые неверные вводы или несанкционированный доступ к системе (безопасность).

С.7 Защищенность

См. приложение F.

С.8 Целостность

С.8.1 Общие положения

В подразделах С.8—С.8.10 обсуждаются некоторые из пунктов, которые необходимо изучить в отношении целостности данных, обрабатываемых системой.

С.8.2 Замена в горячем режиме

Замена в горячем режиме для плат ввода/вывода или модулей должна определяться отдельно, принимая во внимание более высокое напряжение и интенсивность отказов этих устройств.

С.8.3 Диагностика модуля

ОСУ контролирует рабочее состояние каждой платы ввода/вывода или модуля. На человеко-машинном интерфейсе отображается режим как нормальной, так и ненормальной работы, например, отказ или отмена действия.

С.8.4 Проверка вводимых значений

Когда однополюсный переключающий контакт используется в виде двух цифровых вводов, логика проверки осуществляется для выявления аномальных состояний. Аналогичным образом, значения вне предела диапазона аналогового сигнала обнаруживаются, когда сигнал поднимается выше или опускается ниже допустимого диапазона.

С.8.5 Функция повторного считывания

Аналоговые и цифровые выводы ОСУ посылаются обратно на входные платы для выполнения логики проверки. Например, эта функция может быть использована для проверки эмиссии команд открытия/закрытия или значения излучаемых уставок.

С.8.6 Принудительный вывод

В случае отказа или ненормальной работы каждый цифровой и/или аналоговый вывод принудительно устанавливается к предопределенному значению, устанавливаемому индивидуально.

С.8.7 Функции контроля

Входные платы предназначены для обнаружения наиболее распространенных ошибок в поле, то есть открытой или разомкнутой цепи.

С.8.8 Контроллеры

Оценка включает в себя:

- использование запоминающего устройства с произвольным доступом (RAM) с функцией коррекции ошибок;
- подход к устойчивости к отказам/резервированию и связанных с этим вопросами значимости данных, например, гарантии того, что никакие «неверные» данные не могут быть отправлены в поле в случае отказа основного контроллера.

С.8.9 Сети

Оценка включает в себя:

- проверка целостности сообщений, например, коды с коррекцией ошибок;
- временные прерывания на коммуникациях;
- биты состояния, автоматически связываемые со значением так, что приложение может оценивать качество данных.

С.8.10 Рабочие станции и серверы

Оценка включает в себя:

- запоминающее устройство с произвольным доступом (RAM) с функцией коррекции ошибок.

Приложение D
(справочное)

Испытания достоверности

D.1 Общие положения

Испытание внесением ошибки в систему обеспечивает полезный вклад в оценку достоверности систем (технических средств и программного обеспечения).

Данные методы требуют от персонала, проводящего испытания, глубоких знаний функционирования системы, ее физической и функциональной структуры, и часто делают необходимым получение физического доступа к системе.

Концепция этих испытаний состоит в следующем: достоверная система не должна выполнять задачи неправильно, несмотря на отказ элемента системы или попытки проникнуть в систему через ее границу.

Чтобы проверить это, создаются ошибки (чтобы проверить целостность) и/или альтернативное несанкционированное или неправильное действие (чтобы проверить защищенность) и наблюдается результирующее поведение системы (состояние выходов и/или оповещающее выходное сообщение).

Ниже приводятся примеры вопросов, на которые должны быть получены ответы относительно поведения системы когда:

- происходит ошибка, доводится ли выход системы до предопределенного состояния или замораживания?
- экран не работает правильно, блокируется ли клавиатура автоматически?
- связь перегружена, как ведет себя система?
- ошибка внесена, срабатывает ли сигнализация, например, включается «сторожевое устройство», звучит сигнал тревоги, начинают работать соответствующие средства печати?

Чтобы избежать ненужной работы следует на основе аналитического изучения принять согласованный подход к испытаниям, начиная с уровня печатной платы с постепенным переходом на уровень интегральной схемы.

В общем случае вводится единичная неизменяемая ошибка.

Тип вводимых в систему ошибок может быть, например, таким:

- удаление платы или модуля;
- разрыв связей платы (большинство отказов системы из-за неправильных связей);
- нарушение контактов микросхем или принудительное воздействие на них для получения логических 0 или 1.

Для проведения испытания могут потребоваться специальные средства типа:

- расширитель платы с выключателями;
- зажимы;
- специальные программы для испытаний.

В зависимости от глубины оценки, метод может отнимать много времени, но имеет преимущество, связанное с простотой осуществления и относительно недорогими средствами проведения испытаний.

Примечание — Следует соблюдать осторожность и предусмотрительность при проведении этих испытаний, чтобы избежать повреждения каких-либо элементов системы.

D.2 Вводимые ошибки

D.2.1 Общие положения

Классификация потенциальных видов отказов систем приведена в 5.2.3 МЭК 60812:2006.

Далее приведены примеры ошибок, которые могут привести к отказу системы и использоваться для моделирования.

D.2.2 Отказы системы из-за дефектного модуля, элемента или компонента

Системные отказы могут возникать в результате отказов, вызванных возможностями поддержки, высокими температурами, функциональными возможностями, такими как:

- потеря энергоснабжения от единственного источника энергоснабжения;
- потеря энергоснабжения от резервного источника энергоснабжения (как активного, так и пассивного);
- потеря энергоснабжения резервных модулей как с первичной так и с вторичной стороны модуля энергоснабжения;
- потеря энергоснабжения отдельных модулей и элементов;
- потеря модулями и элементами, отдельными и резервными, связи с коммуникационной шиной;
- потеря модуля или элемента;
- потеря энергоснабжения периферийного оборудования (экранов, клавиатур, принтеров, двигателей диска и т. д.;
- потеря связи с периферийным оборудованием;
- обрывы и короткие замыкания в контурах энергоснабжения, шинах связи, адресных линиях, линиях вход/выход.

D.2.3 Отказы системы из-за ошибок человека

Отказы системы могут происходить из-за ошибок, вызванных неправильными действиями персонала при обслуживании, реконфигурации, модернизации программного обеспечения системы, например, таких как:

- перемещение резервных кабелей шины;
- набор неправильного адреса модулей, элементов и т. д.;
- установка печатных плат в неправильном положении;
- установка печатных плат в перевернутом положении;
- установка соединителей в неправильном или обратном положении;
- установка соединителей в неправильном положении;
- непрочные контакты соединителей после ремонта;
- изменение полярности энергоснабжения;
- отказ выполнения полной или корректной инициализации или процедуры запуска;
- повторное использование одного и того же адреса и т. д.

D.2.4 Отказы системы, вызванные неправильными или несанкционированными входами в систему через человеко-машинный интерфейс

Системные отказы могут возникать в результате отказов, вызванных плохой подготовкой, эргономикой, неверным интерфейсом пользователя, таких как:

- вызов или использование несуществующих или неправильных отображений, кодов, программ или периферийных устройств;
- перегрузка клавиатуры или сенсорной панели вызовом большого количества команд в течение короткого промежутка времени (поворот n-ключей);
- использование неполных кодов для вызова отображения, тэгов и т. д.

D.3 Наблюдения

Когда вышеупомянутые ошибки введены, регистрируются следующие вопросы и ответы на них:

- на какие задачи системы и как воздействуют введенные ошибки?
- изменяются ли входные сигналы, пока детектируются все соответствующие модули?
- соответствуют ли выходные сигналы всех модулей правильным сигналам на входе? корректируется ли еще представление данных операторам?
- правильно ли выполняются команды оператора?
- правильно ли функционирует связь между самостоятельными узлами, с ведущим компьютером, с пунктом управления системы, печатающими устройствами и т. д.?
- есть ли задержки (потери времени) действий в каком-либо модуле?
- система сообщает об ошибке?
- автоматически или в течение некоторого промежутка времени?
- автоматически, после периодического испытания?
- на каком уровне системы ошибка была сообщена (пункт управления системы, элемент системы)?
- обеспечена ли система защитными средствами, чтобы избежать возникновения отказа?
- предотвращается ли распространение ошибки?
- продолжается ли действие через резервную связь?
- деградирует ли выполнение задачи системы?
- продолжается ли выполнение операций резервными средствами; ухудшается ли при этом выполнение задач(и) системы?
- достигает ли выход системы установленного уровня в случае неспособности системы продолжать правильное действие?
- действительно ли ремонт в оперативном режиме возможен без воздействия на задачу системы?
- имеется ли сообщение об ошибке, обеспечивается ли однозначная информация относительно отказавшей части системы?
- может ли осуществляться ремонт в оперативном режиме без воздействия или прерывания действия других модулей или элементов системы?
- может ли восстановленный или запасной модуль или элемент автоматически запуститься и правильно функционировать после установки в систему?

D.4 Интерпретация результатов

Для того чтобы облегчить интерпретацию результатов, рассчитывается процент вводимых ошибок, при которых:

- продолжается правильное функционирование;
- срабатывает правильная сигнализация.

Хотя данные не могут использоваться в абсолютном виде, тем не менее, они ценны в сравнительных ситуациях.

Подобный подход применяется для оценки готовности, когда степень компенсации самоконтроля рассчитывается как процент ошибок, обнаруженных самоконтролем.

Приложение Е
(справочное)

Доступные базы данных интенсивности отказов

Е.1 Базы данных

Следующая библиография представляет собой не исчерпывающий перечень в производном порядке источников данных интенсивности отказов для электронных и неэлектронных компонентов. Следует отметить, что эти источники не всегда согласуются друг с другом, и поэтому следует соблюдать осторожность при использовании данных.

МЭК ТР 62380 Справочник данных по надежности. Универсальная модель для прогнозирования надежности электронных компонентов, печатных плат (PCB) и оборудования

Стандарт Siemens SN 29500 Интенсивность отказов компонентов (части 1—14); Siemens AG, CT SR SI, Отто-Хан-Ринг 6, D-81739, Мюнхен

Telcordia SR-332, выпуск 01: май 2001 Методики прогнозирования безотказности для электронного оборудования (telecom-info.telcordia.com), (Bellcore TR-332, выпуск 06)

EPRD (RAC-STD-6100) Данные безотказности электронной аппаратуры. Центр анализа надежности информации, 201 Mill Street, Рим, Нью-Йорк 13440

NNPRD-95 (RAC-STD-6200) Информация о надежности неэлектронных частей, Центр анализа надежности информации, 201 Mill Street, Рим, Нью-Йорк 13440

HRD5 Британское руководство по надежности информации для компонентов, используемых в телекоммуникационных системах, British Telecom

Китайский военный/промышленный стандарт GJB/г 299B Прогнозирование методики безотказности электронного оборудования, (gost.e-ecolog.ru)

ISBN:0442318480 Руководство по безотказности American Telephone & Telegraph Co. (AT&T). Klinger, David J., Yoshinao Nakada и Maria A. Menendez, редакторы, Руководство по безотказности American Telephone & Telegraph Co., Van Nostrand Reinhold, 1990

FIDES: январь 2004 г. Руководство по безотказности данных, разработанное консорциумом ассоциации французской промышленности под руководством Министерства обороны Франции. FIDES предоставляется по запросу на gost.e-ecolog.ru

IEEE Gold book Золотая книга IEEE. Рекомендованные правила IEEE для разработки надежных, промышленных и коммерческих силовых систем. Предоставляются данные о надежности оборудования, используемого в промышленных и коммерческих системах распределения энергии. Центр обслуживания клиентов IEEE, 445 Hoes Lane, п/я 1331, г. Пискатауэй, Нью-Джерси, 08855-1331, США, Телефон: +1 800 678 IEEE (в США и Канаде) +1 732 981 0060 (за пределами США и Канады), Факс: +1 732 981 9667 электронная почта: gost.e-ecolog.ru .

IRPH ITALTEL Руководство по прогнозированию надежности. Руководство IRPH ITALTEL предоставляется по запросу: Dr. G Turconi, Direzione Qualità, Italtel Sit, CC1 / 2 Cascina Castelletto, 20019 Settimo Milanese Mi, Италия. Это версия итальянских телекоммуникационных компаний CNET RDF. Стандарты основаны на одном и том же наборе данных с некоторыми изменениями в процедурах и факторах

PRISM (RAC / EPRD) Программное обеспечение PRISM можно заказать по указанному ниже адресу, или может быть включено в некоторые коммерчески доступные пакеты программного обеспечения надежности: Центр анализа надежности, 201 Mill Street, Рим, Нью-Йорк 13440-6916, США

Е.2 Полезные стандарты, касающиеся отказа компонента

Следующие стандарты содержат информацию в отношении отказа компонента:

МЭК 60300-3-2 Управление общей надежностью. Часть 3-2. Руководство по применению. Сбор данных по общей надежности с места эксплуатации

МЭК 60300-3-5 Управление общей надежностью. Часть 3-5. Руководство по применению. Условия испытаний на надежность и принципы статистической проверки гипотез

МЭК 60319 Представление и спецификация данных о надежности электронных компонентов

МЭК 60706-3 Ремонтопригодность оборудования. Часть 3. Верификация и сбор, анализ и представление информации

МЭК 60721-1 Классификация внешних условий. Часть 1. Параметры окружающей среды и их жесткости

МЭК 61709 Компоненты электронные. Надежность. Стандартные условия для интенсивностей отказов и нагрузочные модели для преобразования

МЭК 62061:2005 Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью

Примечание — Дополнительная информация о режимах отказа электрических/электронных компонентов приведена в приложении D.

Приложение F
(справочное)

Требования обеспечения безопасности

F.1 Физическая безопасность

Физическая безопасность направлена на предотвращение умышленного или неумышленного уничтожения системы человеком с последующим доступом к оборудованию. Предлагаемая ОСУ должна быть оценена на способность поддерживать физическую безопасность.

Общие точки оценки физической безопасности включают в себя:

1) доступ к открытым портам данных на персональном компьютере, например, USB, Ethernet, модемы, последовательные порты и т. д.;

2) размещение оборудования, например, в шкафах или на столах;

3) доступ к материалу внутри шкафа, например, ключи, специальные инструменты, или простая неблокирующая защелка;

4) доступ к данным в закрытом оборудовании, например, о температуре, влажности и коррозии;

5) доступ к аппаратной, например, безопасный вход, мониторинг пространства;

6) контроль за изменениями данных через человеко-машинный интерфейс (ЧМИ), например, блокировка клавиатуры.

F.2 Кибербезопасность

F.2.1 Общие положения

Не смотря на то, что поставщики ОСУ должны обеспечивать поддержку кибербезопасности (включая устранение известных уязвимостей), в конечном счете, ответственность за безопасность в эксплуатации несет пользователь оборудования.

ИСО МЭК 27001 и ИСО МЭК 27002 предоставляют основу для всех стандартов по кибербезопасности. ИСО МЭК 27001:2013, приложение А содержит одиннадцать разделов. В разделах 5–15 в целом описаны необходимые действия по обеспечению кибербезопасности. Информация, приведенная в этих разделах, не является исчерпывающей, и организация может посчитать, что необходимы дополнительные цели управления и контроль.

F.2.2 Политика безопасности

Оценка кибербезопасности системы должна проводиться в контексте политики безопасности пользователя. Политика безопасности должна быть включена в ДТС, описанный в МЭК 61069-2.

Политики безопасности разрабатываются для обеспечения направления и поддержки управлением информационной безопасности в соответствии с бизнес-требованиями, а также соответствующими законами и правилами.

F.2.3 Другие факторы, которые необходимо учитывать

В А.10 ИСО МЭК 27001:2013 перечисляется ряд областей, в отношении которых применяемая система должна оцениваться. Например, система должна быть оценена в отношении того, насколько хорошо она поддерживает:

- менеджмент непрерывности бизнеса;
- управление изменениями, например, способность документировать изменения и делать их отмену;
- разделение обязанностей (ролей) и доступ (разрешения), например, руководитель — оператор; инженер — обслуживание;
- планирование и приемку системы;
- защиту от вредоносной и мобильной программы, например, антивируса, шпионского программного обеспечения (ПО), межсетевых экранов, управление исправлениями, пересмотр операционных систем, белые списки, черные списки и т. д.;
- резервное копирование и восстановление, например, автоматическое или ручное, полное или частичное, локальное или сетевое и т. д.;
- обработку носителей, например, открытый доступ ко всем съемным носителям через все медиа-порты, заблокированные посредством интеллектуальной обработки (только USB от определенных поставщиков);
- мониторинг, например, охранная сигнализация, обнаружение вторжений, работоспособность машины, включая состояние обновления и т. д;
- управление доступом и пользовательское управление, например, использование идентификаторов (карт, паролей, подписей), управление учетными записями (создание, удаление) и т. д.;
- управление доступом к сети, например задокументированные IP-порты, межсетевые экраны в сети, соединение Ethernet отключается, если специально не требуется;
- контроль доступа к операционной системе, например, контроль доступа к утилитам командной строки;
- анализ существенно разных операционных систем для ОСУ от офисных систем в заводе, чтобы минимизировать риск функционирующих вирусов;

- управление доступом к приложению и информации, например, ограничение доступа к определенным приложениям управления процессом на конкретные функции и ограничение управляющих приложений для меньшего количества людей;
- мобильную вычислительную технику и дистанционную работу, например, безопасность беспроводной связи, доступ к мобильным устройствам, управление приложениями на мобильных устройствах;
- криптографические средства управления, например, для шифрования дисковода, шифрование сообщений и т. д.;
- безопасность в процессах разработки и поддержки, то есть, имеет ли поставщик определенную разработку политики безопасности и соблюдает ли ее;
- управление технической уязвимостью;
- менеджмент инцидентов информационной безопасности;
- управление непрерывностью бизнеса;
- соблюдение законодательных требований.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60300-3-2	—	*
IEC 60319	—	*
IEC 61069-1:2016	IDT	ГОСТ Р МЭК 61069-1—2017 «Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 1. Терминология и общие концепции»
IEC 61069-2:2016	IDT	ГОСТ Р МЭК 61069-2—2017 «Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 2. Методология оценки»
IEC 61070	—	*
IEC 61709:2011	—	*
ISO IEC 25010	—	*
ISO IEC 27001:2013	—	*
ISO IEC 27002	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

IEC 60300-3-1:2003, Dependability management — Part 3-1: Application guide — Analysis techniques for dependability — Guide on methodology

IEC 60050 (all parts), International Electrotechnical Vocabulary (available at gost.e-ecolog.ru)

IEC 60050-192:2015, International Electrotechnical Vocabulary — Part 192: Dependability

IEC 60068 (all parts), Environmental testing

IEC 60605-1:1978, Equipment reliability testing — Part 1: General requirements[1)]

IEC 60605-2:1994, Equipment reliability testing — Part 2: Design of test cycles

IEC 60605-3 (all parts), Equipment reliability testing — Part 3: Preferred test conditions[2)]

IEC 60605-4:2001, Equipment reliability testing — Part 4: Statistical procedures for exponential distribution — Point estimates, confidence intervals, prediction intervals and tolerance intervals

IEC 60605-6:2007, Equipment reliability testing — Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity

IEC 60605-7:1978, Equipment reliability testing — Part 7: Compliance test plans for failure rate and mean time between failures assuming constant failure rate[3)]

IEC 60706-4, Guide on maintainability of equipment — Part 4: Section 8: Maintenance and maintenance support planning[4)]

IEC 60801 (all parts), Electromagnetic compatibility for industrial-process measurement and control equipment[5)]

IEC 60812:2006, Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)

IEC 61000 (all parts), Electromagnetic compatibility (EMC)

IEC 61025:2006, Fault tree analysis (FTA)

IEC 61069-6, Industrial-process, control measurement and automation — Evaluation of system properties for the purpose of system assessment — Part 6: Assessment of system operability

IEC 61078, Analysis techniques for dependability — Reliability block diagram and boolean methods

IEC 61123, Reliability testing — Compliance test plans for success ratio

IEC 61165, Application of Markov techniques

IEC 61326 (all parts), Electrical equipment for measurement, control and laboratory use — EMC requirements

IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 62443 (all parts), Industrial communication networks — Network and system security

IEC TS 62603-1, Industrial process control systems — Guideline for evaluating process control systems — Part 1: Specifications

ISO IEC 14764, Software Engineering — Software Life Cycle Processes — Maintenance USA Military Standardization Handbook MIL-HDBK-217 issues A through F, Reliability prediction of electronic equipment

---

[1)] Данная публикация отменена и заменена на IEC 60300-3-5:2001.

[2)] Стандарты данной серии отменены.

[3)] Данная публикация отменена и заменена на IEC 61124:1978.

[4)] Данная публикация отменена и заменена на IEC 60300-3-14.

[5)] Стандарты данной серии отменены.

УДК 658.5.012.7:006.354 ОКС 25.040.40 IDT

Ключевые слова: промышленный процесс, система измерения и управления, определение свойств системы, основная система управления, целевое назначение (миссия) системы, оценка надежности системы, влияющие факторы, свойства системы, методология оценки

БЗ 11—2017/73

Редактор *А.А. Кабанов*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 10.11.2017. Подписано в печать 04.12.2017. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,37. Тираж 27 экз. Зак. 2570.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru